



# Module #6 - Managing digital technology risks





Digital Transformation Learning Modules

Time	Slide #	Script (text and actions)
<b>Making the right technology choices (02:42:15)</b>		
<b>Introduction (02:4)</b>		
00:15	1 	<b>Share screen.</b> Hello and welcome everyone. Thank you for coming along to the sixth session of our series of 7 modules on digital government.
01:00	2 	This is meant to be an interactive session. We'll pause regularly for activities and discussions. But do not hesitate to interrupt us anytime for questions or comments. You can do this either by raising your virtual hand, or by using the chat. Unless you have connectivity issues, I'll ask you to keep your video on. But please stay on mute unless you're speaking.
00:10	3	Today's session is about the role of technology in supporting digital transformation, and the decisions digital government teams have to take to make the most of technology.




00:30	4 	<p>At the end of this training session, you should be able to:</p> <ul style="list-style-type: none"> <li>● Identify the main risks in digital projects</li> <li>● Understand the pros and cons of some key technology and delivery choices</li> <li>● Describe a few risk management approaches to minimise the impact of digital transformation failures</li> </ul>
00:50	5 	<p>This session is structured into 4 parts:</p> <ol style="list-style-type: none"> <li>1. First, how has technology changed these last few years and what does it mean for people and governments?</li> <li>2. Two, what are the main risks in digital transformation projects?</li> <li>3. Three, what are the main technology and delivery choices digital government teams need to make?</li> <li>4. And four, what risk management approaches can help you minimise the impact of digital transformation failures?</li> </ol> <p>Do you have any questions before we start?</p>
<b>1. The new technology landscape (16:00)</b>		
00:30	6 	<p>Fifteen years ago, smartphones (as we know them by today's standards) didn't exist. Fifty years earlier, no one even owned a computer. It feels like technology is progressing faster than ever. And it is. The pace of technological progress - especially in information technology - is speeding up exponentially.</p>
00:30	7	<p>This progress was made possible by a series of 3 landmark technologies that have had a profound impact on</p>





		<p>people and economies: internet, mobile and cloud technologies.</p>
00:30	<p>8/9</p> 	<p>The internet is faster, cheaper, and more accessible than ever.</p> <p>[Trainers to use the latest internet stats for their country]</p> <p>79% of the population of Cambodia were internet users as of 2020, against 14% in 2014 and 32% in 2016.</p> <p>35% of the population of Sri Lanka were internet users as of 2020, against 11% in 2014 and 26% in 2018.</p> <p>This trend has been reinforced by the covid-19 crisis. According to the International Telecommunication Union, the number of internet users in Asia Pacific increased by 24% from 2019 to 2021.</p> <p>Source: <a href="https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf">https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf</a></p>
01:30	<p>10</p> 	<p>And according to the Global System for Mobile Communications Association, at the end of 2020, 1.2 bn people in Asia Pacific were connected to the mobile internet, equivalent to a 42% penetration rate. This means that 42% of people in Asia Pacific have in their pocket a tool with 100,000 times the processing power of the computer that landed man on the moon.</p> <p>Internet and mobile technologies have pretty much changed everything in our lives, from ordering a pizza, to getting the news or to communicating with our colleagues, family and friends. This commoditisation of tech has unlocked a world of opportunities for private companies, and the public sector.</p>
03:00	<p>11</p> 	<p>Another technology that has had a profound impact on the ability of organisations to innovate is the cloud. Thanks to cloud computing, software development is much cheaper and easier. Let's pause here and try to unpack what cloud technologies do.</p>






		<p>The first thing to know is that the clouds you see everyday have nothing to do with cloud computing. The cloud refers to resources such as networks, servers, storage or application services that are accessed over the internet. People who're using their computer to access information are not physically in the same place where this information is stored. This is why you can log in to your Instagram account on a new phone after your old phone breaks and still find your old account in place, with all your photos, videos, and conversation history. Every time you do a search on Instagram, your smartphone sends a request over the internet to a far away server, which then sends back the piece of information requested.</p> <p>So, data stored in the cloud is not thin air. Data stored in the cloud is actually stored in huge data centres spread across the world. These data centres are the home to servers which store organisations' data. Because they need to be at a low temperature to work efficiently, data centres are extremely polluting, and produce over 2% of global carbon emissions.</p> <p>Governments can decide to host their online solutions, and the data associated with it either in the cloud, or on-premise. Let's look at the differences between those two models in more detail.</p>
02:00	<p>12</p> 	<p>Traditionally, organisations used to invest into their own infrastructure. They would have their own servers where they would host their software applications. This means that organisations are responsible for managing and maintaining the infrastructure, sometimes with the help of vendors through maintenance contracts. But at the very minimum, organisations have to manage and plan for replacing or repairing faulty equipment, installing patches and software updates and ensuring that the servers are up and available all the time. On the other hand, organisations keep complete control over their infrastructure. This is what we call on-premise. On-premise means that the total cost of ownership for buying the equipment, software, licences and maintaining the infrastructure rests with the organisation themselves. Usually, on-premise requires a large capital investment to buy the infrastructure upfront. For a government, hosting solutions on-premise means investing</p>



		in their own data centres to host their digital services.
02:00	13 	To illustrate the difference with cloud computing, let's use an analogy. Let us take a utility company. The utility company stores huge amounts of resources like water, electricity or gas, and provides those resources to users when they need them. Whenever you need electricity, you just need to turn on a device or a switch and the provider supplies you with electricity instantly. The supplier will measure your consumption and then charge you for what you consumed. A utility provider is able to supply resources for consumers with small and significant needs. For instance, in the case of electricity, the same provider can supply a very small household as much as a factory or a data centre with much bigger needs. The consumer does not have to worry where the electricity will come from. This is catered for by the utility provider.
04:00	14 	<p>Cloud computing's model is similar to the utilities supply's model. But instead of supplying people with resources like water or electricity, it supplies infrastructure like servers or storage or supplies application services like software or apps. A cloud service provider is able to provide resources like servers or storage on-demand in very small or large sizes. In contrast with on-premise, the consumer of cloud services does not have to worry about buying, managing or maintaining the infrastructure. The onus for that is on the cloud service provider just like it would be for a utility service provider. However, this implies that the organisation has less control over the infrastructure.</p> <p>When you use the cloud, similar to utilities, you pay as you go for what you consume. There are different models but in general you can start by paying for a very small amount for services and then increase your subscription as your need increases. This means that cloud does not require a big initial capital investment as opposed to on-premise but the long-term costs can be higher in some cases.</p> <p>To summarise, cloud services allow anyone to develop online services without big upfront investment in data</p>







		<p>infrastructure. Organisations only pay for what they need, which makes it easy for them to scale their solution. This has considerably lowered barriers to entry to starting an online business (anyone with a credit card can literally have access to cloud computing). This also applies to the public sector.</p>
00:30	<p>15</p> 	<p>But it can be scary for governments to make the jump to the cloud or embrace other recent technology. Because they induce significant changes, large and traditional public sector organisations may think it's too risky for them to take such steps.</p>
01:30	<p>16</p> 	<p>There is also the other extreme where public sector organisations are tempted to adopt new shiny technology just for the sake of it. If the Minister is talking about blockchain, but at the front line civil servants are faxing documents around, something has gone a bit wrong.</p> <p>As we've seen in module 1, creating a mobile app is not always the solution. Investing in blockchain and virtual reality technologies does not make sense if it's just because people talk about them in the media. Technology is an enabler, it's meant to help governments to offer a better experience to their users. It is not an objective in itself. Don't adopt tech just for the sake of tech!</p>
<p><b>2. Digital transformation risks (44:15)</b></p>		
00:45	<p>17</p> 	<p>How can governments find a balance, and invest in technology in a rational and pragmatic way? This is what we'll try to understand in today's session, but before we do this, we need to understand the risks associated with adopting new technology, and digital transformation more broadly. We'll do this by looking at an illustrative case study. But let's start with a quick group discussion.</p>
10:00	<p>18</p>	<p><b>Group discussion</b></p>





	<p><b>Work activity</b></p> <p>Public experience, why people may fear or resist technology projects in the public sector</p>	<p>In your experience, why people may fear or resist technology projects in the public sector?</p>
<p>02:50</p>	<p>19</p> <ul style="list-style-type: none"> <li>Workload</li> <li>Quality</li> <li>Cost efficiency</li> <li>Resilience</li> </ul>	<p>There are lots of reasons why people fear embarking on digital transformation, and investing in technology. Some of these reasons are legitimate. Indeed, digital transformation is risky.</p> <p>We can summarise these risks into 4 categories:</p> <ol style="list-style-type: none"> <li><b>1. Operational:</b> Digital operational risks are risks that result from failure in software or hardware. This may lead to an online service working inefficiently, or not working at all.</li> <li><b>2. Value creation:</b> The operational and value creation risks often go together. Digital value-creation risk arises as part of the delivery of digital services. If services do not deliver the desired results, then there's a loss in value creation.</li> <li><b>3. Cyber and data privacy:</b> The risk of cyber attacks, as discussed in our module about trust, can have extreme consequences. These types of attacks often have the objective of accessing sensitive information and then using that information for malicious acts—for example, extortion and preventing normal services from flowing. Cyber attacks have disrupted some of the world's largest companies as well as government bodies. But the threat is not always external. Because of poor processes or capacities, organisations can provide unauthorised access to personal information.</li> <li><b>4. Reputational:</b> A fourth risk that governments may face in addition to all the other ones we've just mentioned, is the reputational risk. If digital services don't work properly, or if a government's body fails to prevent a cyber attack, then people may lose trust in their ability to do their job.</li> </ol> <p>None of these risks are negligible. Here's an example to illustrate this.</p>





00:30	<p>20</p> 	<p>In 2012, New Zealand’s Ministry of Education launched Novopay, a web-based payroll system used for over 110,000 for teachers employed in 2,500 schools. It was a spectacular and public failure and is probably the country’s most famous IT disaster. What happened?</p>
00:40	<p>21</p> 	<p>The goal of the Novopay project was to replace the existing and ageing payroll system with “a modern, technology-based solution which would provide greater functionality, a better user interface and more useful information.”</p> <p>To bring down costs, the Ministry of Education thought the best thing to do was to find an off-the-shelf payroll system that could be configured and licensed.</p>
01:40	<p>22</p> 	<p>So, in 2008, on recommendation of the Education Minister, the private company Talent2 was awarded a 10-year multimillion-dollar contract to deliver the Education Service Payroll including managing any third parties to support the delivery of the payroll.</p> <p>Novopay was meant to go live in May 2010 but by January, several milestones had not been met and an external review of the project advised the Ministry that the original contract dates were unachievable. The decision was made to continue to work with Talent 2 on the Novopay solution and not to exercise a contract clause that would have allowed termination.</p> <p>The rollout was delayed by more than 2 years. Along the way, the Ministry of Education spent \$650,000 trialling the system before it was rolled out nationally. More than half of the 700 trial-users felt they were not ready for the system to go live but the Government went ahead anyway.</p>
01:40	<p>23</p> 	<p>Novopay went live and performed its first pay run in September 2012. While many of the payees received the correct pay, a significant number did not. 5000 school staff were underpaid (5.05%) and 15 were not paid at</p>





		<p>all. One teacher was paid for 39 days, instead of 39 hours getting thousands of dollars more than he should have. A relief teacher was paid for working at two different schools on the same day. Novopay even took \$40,000 directly out of a school bank account to pay a number of teachers who had never worked there.</p> <p>Concerns were raised that Novopay also committed breaches of privacy by giving teachers' personal information, including bank account details, to the wrong schools. A school principal discovered that a glitch in Novopay allowed staff at a different school to change the pay details of his teachers, showing an opportunity for fraud on a huge scale.</p>
01:00	<p>24</p> 	<p>The 'Novopay debacle' as it was called received almost daily media attention, causing embarrassment for the new Minister of Education, and contributed to the resignation of newly recruited Education secretary Leslie Longstone.</p> <p>By the end of April 2013, the cost to the Government of fixing Novopay had risen to 11 million Australian dollars (USD 8.2) and was still climbing. The Ministry of Education spent an extra AUD 1.7 million (USD 1.3) paying 12 consultants to help sort out problems with Novopay. By the start of 2015, the cost of fixing had risen to AUD 45 million (USD 34).</p>
00:40	<p>25</p> 	<p>In 2016, a report said that although Novopay had improved, user satisfaction was lower than it should be and the system still had significant defects. It said Novopay:</p> <ul style="list-style-type: none"> <li>• used error-prone manual workarounds and required 13,000 manual form entries every fortnight, and</li> <li>• was based on a feature of the Oracle Application Server, which Oracle would not support after December 2019.</li> </ul>
15:00	26	<b>Activity</b>





		<p>According to you, why did the Novopay project fail? What could they have done differently to avoid such a failure?</p>
<p>06:30</p>	<p>27</p> 	<p>Why did the Novopay project fail? Several things went wrong:</p> <p><b>They didn't start with the problem, but jumped to a solution.</b></p> <p>The government wanted “a modern, technology-based solution which would provide greater functionality, a better user interface and more useful information”. This is not a problem, it's a solution. What was the problem Novopay was trying to solve? Having all teachers being paid for their work. How might that goal be achieved? By implementing a payroll system that all schools in New Zealand could use to ensure that all teachers were correctly paid. The key word being repeated here is 'all'. All schools. All teachers. All staff. To meet the needs of 'all' the people, the system would have to understand New Zealand's education legislation and tax rules; it would also have to understand the employment agreements between schools and teachers, and how the people in schools in New Zealand worked and engaged with each other. This is because these are the people who would actually be required to enter data into the system.</p> <p>The Ministry of Education should have begun the project by investing heavily in understanding the people and processes involved. It should have created user-groups, conducted a large volume of insight interviews, developed personas and designed and tested different ways for school admin staff to ensure their teachers were paid. It should have completed all of this insight and user-experience work before going to market to choose software. Instead, it failed to take into account user needs, and when Novopay was launched, thousands of them didn't get paid</p> <p>Another consequence of starting with the solution rather than the project was bad delivery choices: The Ministry of Education went to market, chose and negotiated a contract with an IT payroll vendor with a ready-</p>







		<p>made solution. This was a poor delivery choice. Their problem was too complex for a vendor’s ready-made solution. It required lots of customisation that the vendor wasn’t able to provide. Bespoke development would have made much more sense here. But having agreed to a large multi-million dollar contract, there was no room for the IT company to say, “Actually, we’re not the right people for the job”. This was a fatal mistake: choosing to go for an off-the-shelf solution and deciding on the software provider before determining what was needed.</p> <p><b>They didn’t start small, but went for a big bang launch, despite poor user feedback.</b></p> <p>Politicians decided to launch Novopay in September 2012 while trial users said they were not happy with the solution. A solution is ready to go live when it receives good user feedback, not when the government says so, whatever pressure they may feel from the media or voters. The launch totally failed. Instead of doing a big bang launch at the national scale, they could have decided to focus on a school, or a district. This way, they would have been able to identify errors early on, and fix them before scaling the solution to the national level.</p> <p>Besides, because they didn’t start small, and signed a 10-year multimillion-dollar contract, it made it difficult for them to consider other routes than Talent2 to solve their problem. By starting small - by which I mean agreeing on a limited scope, for a short period of time and a limited budget - they would have been able to test Talent2’s work. Instead of this, they got stuck with a provider that wasn’t equipped to suit their needs. In 2010, because Talent2 failed to provide the solution in time, the Government of New Zealand could have decided to put an end to their contract at no cost. But they had already invested so much money that they decided to continue with them.</p> <p>Eventually, it cost them even more. Years later, in 2016, a report highlighted that Novopay was using error-prone manual workarounds and that it was based on a feature that would no longer be supported by their application server.</p>
--	--	--





01:35	28 	<p>So the Government of New Zealand finally ditched Novopay in 2021 and switched to EdPay. As you can see, they have learned from their mistakes. They engaged with schools early on, and rolled out the solution incrementally, both in terms of features, and audience:</p> <ul style="list-style-type: none"><li>• “EdPay now has most of the functions of the existing forms-based service, and the remainder are being built in stages, once they’re tested and ready.”</li><li>• “We began trialling EdPay with payroll administrators and principals with 11 schools in March 2019, adding a further 15 in May, and increased to 200 in July 2019. Based on their feedback, we offered it to an additional 1,000 schools in September 2019, and rolled it out to the rest before the end of the year.”</li></ul> <p>This allowed them to build a tool that’s simple to use, and answer user needs.</p> <p><a href="https://educationpayroll.co.nz/edpay/">https://educationpayroll.co.nz/edpay/</a></p>
01:25	29 	<p>We’ve just seen that investing in new technology is risky, and that when digital projects fail, they can have significant consequences. Is it better to do nothing then? No. This could be even riskier. Choosing to do nothing actually means choosing to stick with legacy systems. Using ageing systems - or ‘keeping the lights on’ as some people say - brings its own risks:</p> <ul style="list-style-type: none"><li>• Systems may reach a breaking point when they are overloaded with data that they were not designed to handle.</li><li>• Old systems also carry long term security risks as vendors may stop delivering patches for them over time.</li><li>• Another problem is that legacy systems can be hard to change to cater for new user needs. Organisations that don’t innovate will be left behind as technology advances.</li></ul>






<b>Break (05:00)</b>		
<b>3. Making choices (1h10)</b>		
00:20	30 	In this section, we'll look at some important delivery and technology choices governments have to make when planning for their digital transformation.
00:20	31 	The first one is not really a choice, as you may have deduced from the Novopay case study. All digital projects should start by looking at problems, then solutions.
00:45	32 	Not the other way around. Thinking about solutions before you entirely grasp the problem to address, is like having a carriage drawing a horse. This does not work. With Novopay, choosing a solution before understanding the problem led to a waste of time, money and efforts on customising an off-the-shelf software that was not adapted to the specific needs of schools in New Zealand.
00:50	33 	Another challenge which digital teams often face when delivering and maintaining technology across an organisation is that they would like to deliver much more than is possible with the time, money or people they have.  Very often, teams decide to prioritise technology projects based on factors like feasibility, complexity, return on investment and benefit to users. But prioritisation using these factors becomes very challenging when comparing diverse potential investments, for example a new digital service vs. upgrading laptops.
00:50	34	This challenge can be reduced by placing more emphasis on balance over prioritisation of portfolios. Portfolio




		<p>balancing is the idea that teams should consciously choose the balance of their portfolio between different categories of work, before they prioritise it.</p> <p>You may wonder: what categories should we use for technology investment? There's no definite rules, categories may change depending on context. But here are some categories to help you understand what a balanced technology portfolio may look like:</p>
03:00	<p>35</p> 	<p><b>1. Creating or changing technology to gain new value for the organisation or its users.</b> This means investing in completely new projects, for example building a new digital service.</p> <p><b>2. Maintaining the existing technology.</b> This means making sure technology you invested in years ago is still up and running, whether it means paying the host bill each month or fixing minor bugs.</p> <p><b>3. Renewing technology</b> goes beyond fixing minor bugs in the short term. It's about ensuring the long term health of technology, which may involve significant changes for example in architecture, or platform. It could be moving from private data centres to the public cloud..</p> <p><b>4. Enabling the delivery of services.</b> This means investing in technology that does not provide direct value to service users, but those delivering these services, for example investing in building links between applications to allow data interoperability.</p> <p><b>5. Reacting to incidents</b> which occur, from managing incidents to leading investigations and remediate to address the issue.</p> <p>Categorising technology projects allows teams to assess where they need to invest to reach a balanced portfolio. If less than 5% of their budget is invested in creating new products, and over 80% on maintaining technology, there's clearly an issue.</p>



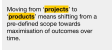

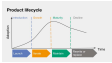
		<p>Having a balanced portfolio allows teams to make better strategic decisions and financial plans. Once they know how much they want to spend in each of these categories - for example 10% of their budget on enabling - then it's easier to decide which projects to fund and not to fund in that category.</p> <p>Let's look at other choices digital teams need to make.</p> <p><a href="https://medium.com/@daverog/sustainable-technology-with-balanced-portfolios-53b496029329">https://medium.com/@daverog/sustainable-technology-with-balanced-portfolios-53b496029329</a></p>
00:30	<p>36</p> 	<p>An important choice government organisations have to make is whether or not to invest in new technology and replace legacy systems. Because funding is always tight in government, it's important to prioritise where money should be allocated in priority.</p>
01:05	<p>37</p> 	<p>Investing in new technology is attractive, but it's not always the right thing to do. It's important to beware of:</p> <ul style="list-style-type: none"> <li>● <b>The attraction of the 'new'</b>. It's very tempting to invest into trendy technology like AI or blockchain. But it may not bring value for money if there isn't a strong business case behind it.</li> <li>● <b>Artificial commercial incentives</b>. Vendors tend to push organisations to invest into new technology but it's often more to their advantage than to their clients. Constructively challenging and weighing options can avoid falling into commercial traps.</li> </ul>
03:25	<p>38</p> 	<p>When is it right to replace legacy systems?</p> <ul style="list-style-type: none"> <li>● <b>When it is soon to be unsupported by the vendor</b> (like Novopay and Oracle). Vendors usually publish 'end-of-life' timings for their systems ahead of time, so that clients have sufficient time to plan for the retirement of their old systems and think about their replacement. This is something that organisations</li> </ul>






		<p>usually do as part of their yearly digital portfolio review.</p> <ul style="list-style-type: none"> <li>● <b>When it becomes too difficult to update or change.</b> A system must be flexible enough to be changed to reflect new user needs or adapt to new requirements (for instance new legal requirements). If changing the system becomes too cumbersome, then it is an indication that it is time to replace it.</li> <li>● <b>When it is no longer cost effective.</b> Sometimes maintaining an existing system costs more than replacing it. This may be because the system is too old or because newer technology is much more efficient and affordable. Either way, if an existing system is no longer cost effective, then it is very sensible to start thinking about its replacement.</li> <li>● <b>When it becomes flaky or inefficient to use.</b> With time, systems may become clunky or slow or difficult to use. This may simply be because they weren't designed to cope with the new circumstances. For instance, they may not have been designed to cater for a high number of users. Their database may not be designed to hold so much data.</li> <li>● <b>When it cannot integrate with other systems anymore.</b> A system may be still working well on its own, but unable to interact with more recently built systems or with systems that it used to interact with but that have been upgraded or changed. If it becomes difficult to do these integrations or the old system does not support them, then it's worth considering replacing it.</li> </ul>
01:00	39 	<p>Irrespective of whether you are investing in a new system or using a legacy one, an important consideration which is often overlooked when planning and budgeting is maintenance. A common mistake is to view digital transformation initiatives as projects that have a defined start and end date. This means that the planning and budgeting is also constrained in time and there is an expectation that once the 'project' finishes, it doesn't require funding anymore. This is one of the reasons why digital systems end up getting out of date over time</p>








		because the maintenance hasn't been planned for.
01:00	40 	Launching a new digital service is just like buying a new car. You may spend a lot of money to buy a brand new car with the latest technology in but that doesn't mean that the car will continue to function well if it isn't maintained regularly. A different way to look at digital transformation is to move away from 'projects' to 'products'. Moving from 'projects to products' means shifting orientation from delivering pre-defined scope towards maximisation of outcomes over time.
02:30	41 	<p>A project-led approach is very much aligned to traditional waterfall projects. Within a project mindset, the assumption is that work is predictable and repeatable. The focus is on meeting defined milestones. Project-led digital transformation is more rigid, there is little room for getting user feedback and accommodating changes. This works well in other sectors for example in construction projects but we have seen in previous modules that digital transformation doesn't really work that way.</p> <p>A product-led approach is often more suitable for digital transformation. A product mindset is outcome-based; the focus is on outcomes more than milestones. It is service-led because it is the service that delivers the outcomes to the users and not the technology. A product-led approach is research driven because there is the awareness that users' needs are what matter the most and what should drive the design. Product-led digital transformation is more aligned with agile ways of working and therefore allows for more flexibility and adaptability. And finally, because it is human-centred, product-led approach continues to optimise for value over the long term because there is a need to deliver outcomes to the users through the lifetime of the product.</p>
01:00	42 	A product as opposed to a project has a longer lifecycle from its inception to its retirement. Throughout the lifecycle, a product requires investment although it typically requires more investment at the beginning. This implies that beyond the initial launching phase, maintenance of the product needs to be planned and budgeted for. At the end of the lifecycle, a decision needs to be taken to either rewrite the product or to replace it.



02:00	<p>43</p> 	<p>Another common technology choice is whether to build or buy? Sometimes it feels safer for government teams to rely on a supplier because if something goes wrong, they think they'll avoid the blame. This is wrong for 2 reasons. First, we saw in previous modules that it's ok to fail, if we learn from our mistakes. Second, it's not because service teams work with suppliers that they should lose entire control over a service project, and therefore responsibility. At the other end of the spectrum, there are teams that would rather build a service in-house to be able to claim credit for it. It's called the 'not-invented here' syndrome. Again, this is not a legitimate argument.</p> <p>The downside of buying technology is the loss of control and flexibility. Any new features you ask from the vendor may require additional time, money and even maybe contract changes. But governments may face challenges to recruit talent to build digital services internally. No organisation builds everything nor buys everything. There is always the right balance to strike for. So how do you choose?</p>
00:30	<p>44</p> 	<p>If you want a cup of tea, you won't make your own kettle. There are certain things that don't make sense at all to build. For example highly commoditised products like Gmail or Outlook. But it's not always that simple.</p>
02:00	<p>45</p> 	<p>Whether to build or to buy technology depends on several things but here are a few important questions to consider:</p> <ol style="list-style-type: none"> <li>1. How important is that technology to your organisation? Is the technology delivering on the organisation's core mission? Or is it more of a commodity that is needed to build or deliver a service?</li> </ol> <p>Organisations would typically want to keep control over technology that is delivering on its core mission but for other things that are less important to the organisation, it may be sensible to buy.</p> <ol style="list-style-type: none"> <li>2. How varied and predictable are the needs? Are the needs known? How often will the requirements</li> </ol>





		<p>change over time?</p> <p>Where needs are known and requirements unlikely to change drastically over time, buying technology can be a good choice. On the other hand, where the needs are varied and unpredictable, building the solution would allow the organisation to make changes more easily and at lower costs.</p>
00:20	<p>46</p> 	<p>Governments are called upon to make build vs buy choices for software (<b>Bespoke vs off-the-shelf software</b>), infrastructure (<b>Cloud vs on-premise infrastructure</b>) but also delivery models for these (<b>In-house capability vs outsourced delivery</b>).</p>
00:40	<p>47</p> 	<p>Off-the-shelf software is a product that you buy and use without customisation – take Microsoft’s Office Suite or Adobe Photoshop for example.</p> <p>Bespoke software is designed and built on demand with a specific purpose in mind for the organisation that has commissioned the build.</p> <p>When do you buy off-the-shelf software, and when do you develop your own from scratch?</p>
05:30	<p>48</p> 	<p>It makes sense to buy off-the-shelf software when the need is for something very commoditised and widely available and common. For example products like Gmail or Outlook. There is very little point in re-building these from scratch. Being able to understand what’s commoditised and what’s not requires a good understanding of the market.</p> <p>On the other hand, it’s often better to develop bespoke software when:</p> <ul style="list-style-type: none"> <li>You need to keep control over the software because it’s really important to your organisation or shapes</li> </ul>





		<p>the users' interactions with the government. For example, an online vehicle registration service or online passport application.</p> <ul style="list-style-type: none"> <li>• You're not sure about the needs it's meant to answer, for example a citizen engagement platform. If you anticipate that you'll learn about needs as the project goes, and that you'll have to add new features to your service, then it's better to opt for a bespoke solution. It will be easier and cheaper to make changes..</li> <li>• The needs are varied, like in the case of Novopay. There were too many different types of contracts and scenarios for the Novopay solution to cope with.</li> </ul> <p>The choice between off-the-shelf and bespoke software is not binary. You can also opt for an hybrid approach, where an off-the-shelf solution is partly customised to fit needs that are specific to you. This only makes sense if there is not too much customisation to do. Otherwise you lose all the advantages of an off-the-shelf solution like in the Novopay case study. And it becomes "fake" off-the-self. Off-the-shelf software is meant to be software that you can buy and easily customise, to some extent. More advanced configuration work means spending additional money, time and effort. Besides, because the off-the-shelf solution is owned by an external vendor, you won't be able to reuse all your configuration work if you decide one day for some reason to change the software provider. Because you've invested so much at this point, you're often reluctant to change and found yourself stuck with a provider. This is what we call vendor lock-in. And one day, if the off-the-shelf software stops supporting the features you've developed, all your work may be lost. In a nutshell, digital teams should buy off-the-shelf software only when they know they'll use the software in its vanilla version, with no or very little configuration.</p> <p>In any of these cases, it's important for governments to have an in-house team with the right expertise to make these decisions.</p> <p>Additional reading: <a href="https://governmenttechnology.blog.gov.uk/2014/04/16/guest-post-mapping-the-way-to-a-">https://governmenttechnology.blog.gov.uk/2014/04/16/guest-post-mapping-the-way-to-a-</a></p>
--	--	--





		<a href="https://sboots.ca/2020/09/16/fake-cots-and-the-one-day-rule/">strategy/ https://sboots.ca/2020/09/16/fake-cots-and-the-one-day-rule/</a>
01:45	49 	<p>One frequent question linked to bespoke and off-the-shelf software is when to use open source software?</p> <p>Proprietary software is also known as non-free or closed-source software. It's software that is copyrighted, which means it can only be obtained by paying for a licence.</p> <p>Open-source software, on the other hand, is software that's published in the open under an open source licence, which means it's free for anyone to reuse it.</p> <p>If you are considering using an off-the-shelf open source software, then you need to properly evaluate it as we have just discussed to see whether it meets the needs of the organisation without requiring too much configuration.</p> <p>Open source software is usually useful when building a bespoke software because it provides reusable components which can help to reduce development time.</p>
02:15	50 	<p>Let's take an example to illustrate this. When they build a service, developers don't have to start from scratch. They can use other people's code for specific parts of their service they're building in order to gain time. For example, let's say a software developer is coding an online solution for parents to register their children at school. The solution requires a notification system, to tell parents when their application is being processed, approved or rejected. Notification systems are something that lots of online services need, and therefore can be reused. This is what we call building blocks. If the code behind these building blocks is published in the open, and available for reuse without fees, under an open source licence, then they're open source building blocks. Using open source building blocks allow digital service teams to spend less time coding, and more time focusing on solving the problem at hand.</p>

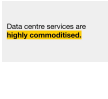




		<p>This is what happened with Notify. The Notify system was developed by the UK government to allow digital service teams to include a notification feature to the services they were developing. It published the Notify system under an open source licence, and since then Australia and Canada have reused it.</p>
01:00	<p>51</p> 	<p>Another example is Singapore’s open source building block for developing forms (FormSG). FormSG allows government agencies to quickly build new forms and workflows by reusing existing code. More than 300,000 digital forms have been deployed using FormSG to date. During the Covid-19 pandemic, FormSG was used to quickly develop workflows for digital services including antigen rapid testing or national Covid financial relief.</p> <p>Source: <a href="https://govinsider.asia/digital-gov/sonjia-yan-product-manager-open-government-products-singapore-women-in-govtech-2021/">https://govinsider.asia/digital-gov/sonjia-yan-product-manager-open-government-products-singapore-women-in-govtech-2021/</a></p>
02:00	<p>52</p> 	<p>Open source software is widely used in large organisations. In a survey the company Red Hat did in 2022, 95% of the leaders they surveyed said that 95% of respondents say that open source was important to their organisation’s overall enterprise infrastructure.</p> <p>Source: <a href="https://www.redhat.com/en/resources/state-of-enterprise-open-source-report-2022">https://www.redhat.com/en/resources/state-of-enterprise-open-source-report-2022</a></p> <p>What are the advantages of open source software?</p> <ul style="list-style-type: none"> <li>● It can help avoid vendor and technology lock-in, where you’re stuck with a vendor or a technology, and can’t change easily, even when it’s the right thing to do. For example, let’s say a team is building a service on a proprietary platform, and wants to change this platform, because a competitor is now cheaper, or because it does not offer all the features they need. To change this, they would need to re-architect their application and completely rewrite it on another application.</li> <li>● Open source offers more flexibility and control over how services are developed and delivered.</li> </ul>




		<ul style="list-style-type: none"> <li>It allows governments to freely reuse solutions across teams, organisations and countries, saving time and money on procurement.</li> </ul>
02:00	<p>53</p> 	<p>Open Source provides building blocks to developers to build services faster. Open source components can play an important role in the foundational layer of a service and it is now very unusual for a development team to build everything absolutely from scratch. But open source components don't just plug and play, especially in the context of services with complex requirements.</p> <p>Open source is not free, and may not save costs overall. There is a common misconception that open source is free. But while the code may be open, there are other costs associated with open source.</p> <ul style="list-style-type: none"> <li>Some vendors provide a free standard open source version of a product, but then charge for additional features or support services.</li> <li>And implementing open source software is not free, governments need teams with sufficient technical expertise to do this. They need to have the right skills in-house to implement open source software, and maintain long-term ownership over the solution built with open source building blocks.</li> </ul> <p>Additional reading: <a href="https://public.digital/2021/06/21/open-source-in-government-creating-the-conditions-for-success">https://public.digital/2021/06/21/open-source-in-government-creating-the-conditions-for-success</a></p>
01:00	<p>54</p> 	<p>An early decision that governments need to make for each new digital service is where to host it. We have covered the differences of cloud vs on-premise infrastructure in the first section of this module as well as the associated benefits. We'll now discuss the key considerations to have when opting for cloud and how cloud transforms the way teams approach delivery.</p>






00:30	<p>55</p> 	<p>Today, data centre services are highly commoditised. Well-established providers like Amazon Web Services or Oracle are able to provide scalable, secure and affordable services. It's hard to match their standard if you are contemplating building your own data centre.</p>
03:00	<p>56</p> 	<p>Using the cloud has many benefits.</p> <ul style="list-style-type: none"> <li>• As we've seen earlier, storing applications and data in the cloud allows digital teams to scale up or down their storage needs on short notice.</li> <li>• They don't need to invest in infrastructure, which requires significant upfront costs. Instead, they only pay for the space that they use.</li> <li>• They don't need IT experts on-site to maintain their servers.</li> <li>• Large cloud services providers often invest significant amounts of money in cybersecurity, which makes their servers secured, and reliable. Lots of governments misunderstand the risks of cloud, and assume it's higher risk. They create a culture of saying everything is 'highly sensitive' or related to 'national security'. Managing risk in the cloud can be hard at first, because it's new, but over time it's cheaper and easier to manage data safely in the cloud. This is because vendors manage the risk of the infrastructure, leaving it your responsibility to only manage the risk of your data and services.</li> </ul> <p>But this doesn't mean cloud services are the go-to solution for all types of data. Governments, like financial institutions, can decide to keep extra sensitive information on-premises to keep control over the security and privacy of the environment, for matters of digital sovereignty.</p>
04:00	<p>57</p> 	<p>Let's say your department is about to launch a new online service, and it has decided to do it on the cloud. What should it look out for?</p> <p><b>Cloud policy:</b> The first thing to verify is whether your government's policies or standards in place allow the use</p>





		<p>of cloud services. Maybe your government has a cloud policy, maybe it's mentioned in other policy documents, like a cyber security policy.</p> <p><b>Data protection:</b> Once you know you can use cloud services, you need to decide on a provider. It's important to look at the data protection measures they have in place. You need an organisation that provides services compliant with the data protection laws in your country. You also need to ensure that they have adequate provisions for protecting unauthorised access to your data from third-parties, including their personnel and other customers.</p> <p><b>Sensitivity of data:</b> Even if you're happy with the data protection measures of your cloud services provider, there may be some data that you find too sensitive to host in the cloud, for example if it's a matter of national security.</p> <p><b>Service level agreements:</b> another important aspect to consider before contracting with a cloud service provider is the level of service which they're able to guarantee. Most cloud service providers now provide services with high availability. But it's important to do a proper assessment when deciding to move a service to the cloud. For instance, if a service is mission critical does it really make sense to move it to the cloud? Even if the cloud service provider is able to provide high availability services, will all the users be able to access the service if for instance some users have poor internet connectivity? These are important things to consider.</p> <p>Additional reading: <a href="https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations">https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations</a></p>
01:00	58 	In 2016, the Government of Philippines announced a cloud-first policy for all federal and local government organisations. The policy aimed at optimising government spending on infrastructure while saving time for delivery of digital services. Rather than focusing on building infrastructure, the government decided to focus its







		<p>efforts on delivering online services. Philippines' cloud policy acknowledged security considerations and recommended contracting with different cloud providers depending on the level of sensitivity of data.</p> <p>Source: <a href="https://govinsider.asia/digital-gov/philippines-announces-cloud-first-policy-for-all-federal-and-local-government/">https://govinsider.asia/digital-gov/philippines-announces-cloud-first-policy-for-all-federal-and-local-government/</a></p>
01:30	<p>59</p> 	<p>On top of the advantages cloud brings in relation to infrastructure itself, cloud can truly transform the way that digital teams approach building a new digital service. First, it allows them to focus on user needs and the design first as they don't need to think about the infrastructure needs upfront. These can be looked into later during the project once they have a clearer picture of what the digital service will look like as cloud providers can pretty much provide infrastructure on-demand. Secondly and perhaps more importantly, opting for cloud frees up technologists and experts allowing them to be part of the digital teams and focus on delivery.</p>
00:30	<p>60</p> 	<p>Build vs buy decisions whether for software or for infrastructure have a direct impact on the choice of delivery models. Usually building software or infrastructure requires more in-house capability while buying implies some level of outsourcing.</p>
03:30	<p>61</p> 	<p>Government teams can decide to go for an insource model - consists in delivering a service project entirely in-house, without the help of any external supplier - or an outsource model - consists in entirely buying services and products from the market.</p> <p>But they can also go for a hybrid 'bridge' model, where service teams lead on projects, but bridge capability gaps in-house with expertise and/or products from the market.</p> <p>The choice of a delivery model is closely linked to build vs buy decisions for software and infrastructure. Where the new service being created is really core to the organisation mission or where the needs are unpredictable and frequent changes will be required, it is best to build internal capability. Ownership and control is another</p>



		<p>key consideration to decide when to outsource or not. How important is it for the government team to retain direct ownership and control over the development of the service, for example due to political or security reasons?</p> <p>Ideally, there would be a one-to-one mapping between build vs buy decisions and the choice of the delivery model: in-house capability for services that are built and outsourced for the ones that are bought. But it may not always be that straightforward in practice because governments may lack internal capability. Sometimes, the government team may not have the skill sets and the bandwidth to develop the service. It might also be difficult to acquire the skills or hire new talent within reasonable timeframes. In those situations, the team may need external help from a supplier. If external help from a supplier is required to build a service for these reasons, then a hybrid model can be considered but complete outsourcing is not recommended.</p>
02:00	<p>62</p> <p><small>A digital service requires long-term ownership and should be treated as a product.</small></p>	<p>Outsourcing delivery makes sense in the case of infrastructure if the choice has been made to go for cloud. However, in the case of software, it is more tricky to completely outsource delivery. A digital service should be treated as a product rather than a fixed-term project and therefore it requires long-term ownership. Users' needs will change over time as well as technology. The service itself will mature and the solution will need to be updated and refreshed to reflect those changes. If the delivery is completely outsourced, you may end up being locked with a vendor over a very long period of time. So even in cases where delivery needs to be outsourced, it is always advisable to have a minimum in-house capability that can oversee the work of suppliers and work alongside them.</p>
15:00	<p>63</p> <p><small>Write group discussion</small></p>	<p><b>Group discussion</b></p> <p>Think about your organisation. What good technology choices has it made? And what do you think could have been done differently?</p>






4. Risk management (25:15)		
a. Do's (19:50)		
00:30	64 	In this last section, we'll share with you some do's and don'ts that can help digital service teams limit the consequences of failures. So that they don't end up with stories like Novopay.
15:00	65 	<b>Group discussion</b> We've all been part of projects that didn't work. Think about a time when you were involved in a project or initiative that failed or was not as successful as you hoped. Why did that happen?
00:50	66 	One thing to know about digital projects is that things will go wrong. It's a guarantee. Digital government teams should not start from the assumption that they're going to build fault-free solutions. What they need is a safe space to fail, a space where they can experiment with small failures with which they can cope with. Organisations who are able to create such environments will avoid Novopay-like disastrous situations.
00:45	67 	As seen in module 3, and with the Novopay case study, it's important to implement services incrementally. In the past, it was more difficult to do. But with modern technology, it is cheaper and easier to try new things. Starting small, testing and then scaling up is one of the best ways to reduce the risk of a new system not working as expected.
01:00	68	Technology projects can be considered 'too big to fail' when they're under political or media scrutiny, when lots of money has been spent on them, or when suppliers' contracts have been made in such a way that it's





		impossible to break them. The challenge when such a scenario arises, is that if somewhere down the line things go wrong, the government ends up spending money without any value in return. It's important to keep options open, by starting small. Starting small and being bold can go together.
00:45	69 	Again, failures will happen. Promoting a learning culture in your organisation is the only way to make the most of these mistakes. If people feel comfortable to share mistakes and discuss them openly within their team, then the team is less likely to repeat the same mistake in the future. Holding regular retrospectives is a good way of encouraging a learning culture within the team.
01:00	70 	One of the risks in some longer term digital transformation is that there can be lots of changes including changes in leadership during the implementation. If change is not properly managed, this can cause the initiative to fail. This is why it is important to balance buy-in from political leaders and buy-in from administrative leaders that are more likely to be there for longer. In the next module, we will discuss some tips for managing change in more detail.
<b>b. Dont's (05:25)</b>		
00:10	71 	And to finish this session, a few things to avoid.
01:10	72 	When a new technology arises, its novelty attracts people, it gets a lot of media coverage and vendors quickly put it at the forefront of their offer. Governments may be tempted to try it out too, or even feel pressured to do so. Like with AI, blockchain and robotics. There is no harm in trying a new technology if it's problem-oriented, if the team starts small, and the organisation has a balanced portfolio of technology projects. But again, if the Minister is talking about blockchain, and at the front line civil servants are faxing documents around, something



		has gone a bit wrong.
00:35	73 	Technology is not the answer to every problem. There are cases where a manual solution is better. Teams need to be pragmatic in their choices. And never automate a process that is wrong in the first place. If a manual process is wrong, automating it will only result in a digital solution that’s wrong.
01:15	74 	While supportive leadership is an extremely important factor and one of the preconditions for successful digital transformation, equally as important is the role of ‘doers’. Digital teams truly are the cornerstone of building a modern digital organisation. Supported by effective governance, they are the muscles that enable an organisation to be responsive, open, efficient and flexible, and to successfully deliver ever more transformational services.  Irrespective of the tech choices governments make, they will need a minimum amount of in-house capability or team to help with making the right choices. Even government organisations buy systems, they need a team that helps identify the needs and write good requirements for tender documents.
00:55	75 	We’d like to conclude with this phrase from Professor Francesco Mancini, from the Lee Kuan Yew School of Public Policy: “Many governments already recognise the importance of technology. But [...] the big challenges are not technical.” What you need to remember from this module is that having a balanced portfolio of technology projects is important, but technology is only one aspect of digital transformation, and without the right culture and processes, it can’t achieve much. This is the main challenge governments face.  Source: <a href="https://govinsider.asia/inclusive-gov/lkyspp-francesco-mancini-what-leadership-looks-like-today/">https://govinsider.asia/inclusive-gov/lkyspp-francesco-mancini-what-leadership-looks-like-today/</a>
01:00	76	Takeaways:



		<ul style="list-style-type: none"> <li>● Internet, mobile and cloud technologies have reshaped the way governments build and deliver services.</li> <li>● Governments have much to do, with limited time, money and people. It's therefore important for organisations to develop a balanced portfolio of technology projects.</li> <li>● For each project, they need to make tactical decisions: on-premises vs cloud, new vs legacy systems, off-the-shelf vs bespoke software, proprietary vs open source, in-house vs outsourced delivery</li> <li>● Whatever they decide, failure is likely. To manage risks, they need to start small, and iterate.</li> </ul>
00:30	<p>77</p> 	Next module: navigating barriers to digital government